IGAM.005A PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Rolf E. Carlson	Group Art Unit 2136
Appl. No.	:	09/698,507	
Filed	:	October 26, 2000	
For	:	CRYPTOGRAPHY AND CERTIFICATE AUTHORITIES IN GAMING MACHINES	
Examiner	:	Brandon S. Hoffman	

DECLARATION UNDER 37 C.F.R. § 1.131

1. This declaration is to establish invention priority of the above-referenced U.S. Patent Application No. 09/698,507.

2. I, Rolf E. Carlson, am the sole inventor of the claims in the above-referenced application.

3. I have reviewed the Office Action from the Examiner at the Patent and Trademark Office dated January 13, 2005 rejecting the claims of the above-referenced application under 35 U.S.C. § 103.

4. On October 26, 1999, I caused to be filed a provisional application, no. 60/161,591 ("priority application"), to which the above-referenced application claims priority. The priority application fully discloses the claims of the above-referenced application.

5. I, the sole inventor, had conceived of the invention at least as early as June 18, 1999 in this country, as described and claimed in the application, and diligently worked with my patent counsel to prepare and file the priority application, including during the critical period between June 18, 1999 and October 26, 1999, as evidenced by the following events:

   a. Prior to June 18, 1999, I emailed a copy of a disclosure paper describing the concepts of the above-referenced application to Bob Dorr, an attorney at the law firm Dorr, Carson, Sloan, & Birney. Appendix A is copy of the email and copy of the attached paper.

   b. To my knowledge, prior to June 18, 1999, after internal review and discussion of the content of the disclosure paper, Charles McCrea, Executive Vice President and General Counsel of Mikohm Gaming Corporation, the initial assignee of the priority application, directed Mr.

Dorr to proceed with preparation of the priority application. Appendix B is a redacted copy of the email directing Mr. Dorr to proceed.

c. Prior to June 18, 1999, I received a letter from Mr. Dorr confirming that he would proceed with preparing the priority application and corresponded with Mr. Dorr regarding background materials and materials disclosing the subject invent. Appendix C is a copy of an email that I sent to Mr. Dorr informing him of the package and his response.

d. Between at least June 18, 1999 and September 30, 1999, I regularly communicated via email and telephone with another attorney, John Thompson, who was preparing the priority application under Mr. Dorr's supervision, regarding questions that arose during preparation of the priority application. Appendix D includes copies of representative such emails.

e. Shortly after it was mailed on August 25, 1999, I received a copy of the first complete draft of the priority application from Mr. Thompson. Appendix E is a copy of the letter enclosing the draft.

f. Shortly after it was mailed on October 13, 1999, I received a revised draft of the priority application.

g. To my knowledge, the application was filed on October 26, 1999 after my review of the revised draft.

<u>Penalty of Perjury Statement</u>

I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful, false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful, false statements may jeopardize the validity of the application or any patent resulting therefrom.

Dated: 7-1-05

By: ______________________
Rolf E. Carlson

From: "Rolf Carlson" <rolfc@swcp.com>
To: "Robert Dorr" <bobdorr@sni.net>
Subject: Modified Alcorn Keene and UGE
Date: Fri, 12 Feb 1999 08:59:38 -0700
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook 8.5, Build 4.71.2173.0
Importance: Normal
X-MimeOLE: Produced By Microsoft MimeOLE V4.72.2106.4

Here is version 0.2

Rolf
Attachment Converted: "c:\eudora\attach\Certificate Authorities for Gaming Services.doc"

Certificate Authorities for Gaming Services

Rolf Carlson
Spring Creek Technologies, Corp.
(505) 256 7647

Abstract

Increasingly, information security technologies will be applied to gaming. It will be necessary to have a certificate authority mechanism in order to support the information security services required for a trusted relationship between the player, house, and game owner. This document describes the required information services along with the certificate mechanism that will be required for the support of such information services in a gaming environment.

In support of the certificate authority, several new uses for authentication and encryption will be introduced, as well as the new utilization of the ITU-T X509 authentication framework.

The consequence of the new gaming information system is a cryptographicaly secure relationship between physically located gaming machines in a casino. Such a relationship will also allow casino games to be seemlessly extended to the Internet using cryptographically secure means. In particular, there is no certificate authorities in use by casinos and local games.

Introduction

In order to achieve a framework that satisfies the information security goals associated with modern gaming and electronic commerce, there needs to be an infrastructure that can maintain a collection of keys. Modern cryptographic functions rely upon keys to protect and unprotect information. More generally, cryptographic protocols and primitives use these keys to achieve each of the information security objectives. Because of the way digital information can be replicated without owner consent, the keys should be regarded as the secret. If this is the case, we now have a new problem of where and how to store the keys so that the information the keys protect is not compromised.

Until about 1974, the primary means for encrypting information to protect privacy used symmetric key techniques. Soon after, however, it was observed that public-key methods could solve the key update problem between two users that know each other. Getting two strangers to have confidence in the identity of each other and content of a transaction, however, was soon seen to be a problem. Digital signature and certificate authorities often rely upon public key cryptography and were developed to solve some of the problems that untrusting parties face when engaging in digital commerce. In the next section, we generally define symmetric and public-key methods, their relative strengths, and weaknesses.

Information Security Goals

There are three goals of information security that are facilitated by cryptography: privacy, authentication, and non-repudiation. Providing a collection of services that satisfy these goals has been generally regarded as a necessary condition for a successful digital framework for electronic commerce. We make the same assumption about electronic gaming.

Privacy

Confidentiality or privacy is the condition where information is kept secret from all but those authorized to know the information. Encryption techniques will be used to ensure confidentiality. It should be noted that encryption does not necessarily provide authentication. Privacy can apply to individuals as well as information. Anonymous WWW surfing is an example of a problem requiring identity confidentiality. Game players may require that their identity not be divulged as a precondition for play. Confidentiality provides this service.

Authentication

Ensuring the identity of communicating parties to one another is called user authentication. Ensuring the content, integrity, origin, date of origin, time sent and other attributes of a message is called message authentication. Authentication will be provided by combining hashing techniques with other cryptographic primitives to form more complicated structures called protocols.

Non-Repudiation

Preventing a party from denying previous actions or commitments is known as the non-repudiation problem. The digital signature can be used to verify the identity of participants in a transaction and later enforce non-repudiation. A casino will need the services of non-repudiation if it is to enforce payment by players that have wagered and lost.

Public and Private Keys

Symmetric-key cryptography, also known as secret-key cryptography, uses a unique key to exchange information between two parties. Therefore, the sender and the recipient of a message must share a secret, namely the key. The difficulty with this approach occurs when a key is compromised or when the parties would like to introduce a new key. This is known as the key-update problem. A well known secret-key cryptography algorithm is the Data Encryption Standard (DES), which is used by financial institutions to encrypt PINs (personal identification numbers).

Asymmetric-key cryptography, or public-key cryptography, by contrast uses two different keys for each participant in a transaction. The asymmetric key pair consists of a public and private-key. The two keys are mathematically related so that data encrypted with either key can only be decrypted using the other. The public-key is made available to the world, while the private-key is kept secret. Entities desiring to send information to a particular individual will obtain the individual's public-key and encrypt information with that key. Only the holder of the private-key can then decrypt the information. This assurance is dependent upon not disclosing the private-key to anyone else. The essential feature of a public-key cryptosystem is that *knowledge of a public-key does not provide any computational information about the private-key*. One well-known public-key cryptography algorithm is RSA (named after its inventors Rivest, Shamir, and Adleman).

Cryptographic Background Art

This section lists four patents that provide the foundational art for public-key cryptography.

Patent number 5,231,668, the Digital Signature Algorithm (DSA). The DSA patent discusses signature schemes in a public-key context.

Patent 4,200,770, the Diffie-Hellman. The Diffie-Hellman patent is an important public-key patent and the described methods are often used for exchanging keys privately over a public network.

Patent 4,405,829, the RSA patent. The RSA patent describes the de-facto standard for public-key encryption around the world.

Patent 4,995,082, the Schnoor identification scheme. Schnoor developed an identification scheme that was later improved by the DSA patent. This patent then becomes prior art for the DSA patent.

Certificates

A certificate authority (CA) is a trusted third-party organization or company that can issues digital certificates used to create digital signatures and public-private key pairs. A public-key (CA) is required whenever a distributed application makes use of public-key cryptography. There are symmetric-key certificate authorities, but we will not consider them in this document. The term certificate authority, or CA, will be used to mean public-key certificate authority. The role of the CA is to guarantee that identity of the individual granted a unique certificate. Usually, this means that the CA has an arrangement with a financial institution, such as a credit card company, which provides it with information to confirm an individual's claimed identity. CAs are a critical component in data security and electronic commerce because the CA can be used to guarantee the identity of two parties exchanging information.

Simple Authentication

Strong Authentication

Certificates

A Heirarchy of Certificate Authorities

Alcorn 086'

The Alcorn 086 patent describes a public key authentication program for verification of the contents a hard disk and therefore a stored game. The use of authentication and encryption programs are not used for the confidentiality and integrity of the digital information that is transferred back and forth between gaming machines, such as a slot machine and a casino server. As such, the present patent describes new art.

Keene EP 0843 289 A2

1. Action Item for Bob: We need an engineer to look at figures 2A, 2B, and 4, 5 to ensure that they somehow don't do what we are suggesting with the array.

2. Action Item for Me: Discuss Blum-Micali

The Keen patent uses a noise diode to facilitate the generation of random numbers. These random numbers are then used in game play. There are well-documented difficulties with obtaining randomness from physical noise sources, such as zener diodes. The problems with these physical sources of randomness include bias and correlation in the output bits [1]. Despite their shortcomings, there are advantages to physical noise sources as opposed to deterministic pseudo-random number generators. One advantage is that no seed is required. Another advantage is that a higher sampling rate can be achieved. We will examine two classes of problems that require random number generation in gaming: seed generation, and sequence generation.

Pseudo-random number generators from deterministic algorithms require a seed, or initial value. Random seeds to be used in a random number generator must be chosen with care otherwise there is a danger that any dependence in the bits of the seed can become amplified in the bits of the pseudo random number generator and lead to an adversary discovering information about the sequence that is used in a game. We discuss a scheme where a collection of physical sources can be used either as a seed for a pseudo-random generator, or simply as a generator for a sequence of random numbers. There is no need to provide seeds for systems that incorporate such number generators, thus simplifying the complexity of maintenance of the gaming machines.

A first solution to the problem of using physical sources of randomness that exhibit bias for random number generation, is to use process 700 from the Universal Gaming Engine to filter the bit streams that exhibit noise and correlation. One advantage of using the UGE filtering mechanism embodied in process 700 is that the device user can then decide on what time scale they would like to obtain stationarity in the output distribution. Using process 700, it is possible to verify that the output sequence of random numbers that will be used later in game play satisfy a collection of criteria that becomes a measure for the quality of the numbers. This measure is often noise generated numbers are statistically random. Having an apparatus such as given in process 700 of the UGE patent (fig. 7) should be a requirement of each random number system approved by a gaming commission. One difficulty, however, with using process 700 of the UGE to filter out correlated or biased sequences is that if the generator does exhibit sufficient bias then play might halt due to a shortage of random numbers.

A further improvement in the solution to this problem of using physical sources for randomness is found in the arrangement of the physical sources. By organizing several physical sources into a particular model we can take the output of the physical sources of randomness, considered semi-random sources, and produce a high quality output of randomness: a quasi-random source. It has been shown that such quasi-random sources can be used in place of truly random ones for applications such as random number generation and random number seed generation [2].

Suppose that we have a source of some randomness that exhibits a bias that is greater than δ and less than $1-\delta$ for some positive number $0<\delta<1$. Let us define a semi-random source as one in which the frequency of the 0's and 1's drifts over time with this bias. Zener diodes fall into the category of semi-random sources.

One construction of a quasi-random source from a semi-random source proceeds as follows. Let n be the input and suppose that we have k independent semi-random sources. Suppose that we then generate the following collection of bit lists:

$$\begin{array}{cccc} X_{11} & X_{12} & \cdots & X_{1n} \\ X_{21} & X_{22} & \cdots & X_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ X_{k1} & X_{k2} & \cdots & X_{kn} \end{array}$$

Let Y_i = Parity $(X_{1I},X_{2I},\ldots,X_{ki})$ then the output $Y_1, Y_2, \ldots, Y_n$ is quasi-random. Even though such a sequence generates a high-quality source of randomness, it is still beneficial to ensure the integrity of the system by passing the resulting stream through process 700 of the UGE.

The solution that results does not significantly raise the hardware costs and needs only focus on ensuring the physical independence of the k semi-random sources by isolating the sources from electromagnetic interaction.

[1] J. Von Neumann, Various techniques used in connection with random digits (notes by G.E. Forsythe), Applied Math Series Vol. 12, pp. 36-38, 1951; National Bureau of Standards, Washington, D.C., reprinted in "Collected Works", Vol. 5, 768-770, Pergamon, New York, 1963.

[2] M. Santha and U. Vazirani, Generating Quasi-random Seque3nces from Semi-random Sources, Journal of Computer and System Sciences 33, 75-87 (1986).

From: "Rolf Carlson" <rolfc@swcp.com>
To: "Robert Dorr" <bobdorr@sni.net>
Subject: Modified Alcorn Keene and UGE
Date: Fri, 12 Feb 1999 08:59:38 -0700
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook 8.5, Build 4.71.2173.0
Importance: Normal
X-MimeOLE: Produced By Microsoft MimeOLE V4.72.2106.4

Here is version 0.2

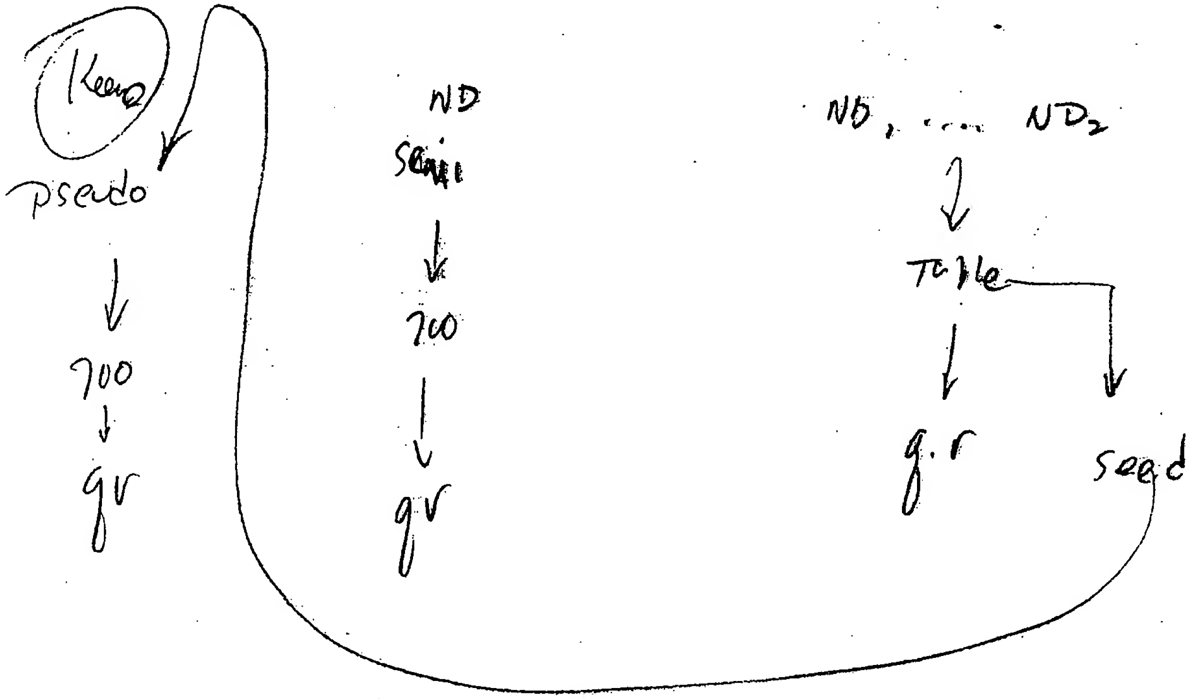
Rolf
Attachment Converted: "c:\eudora\attach\Certificate Authorities for Gaming Services.doc"

paper
psedo
quasi
semi

1990's

paper
noise diode
semi
quasi

PY = 1990



Certificate Authorities for Gaming Services

Rolf Carlson
Spring Creek Technologies, Corp.
(505) 256 7647

Abstract

Increasingly, information security technologies will be applied to gaming. It will be necessary to have a certificate authority mechanism in order to support the information security services required for a trusted relationship between the player, house, and game owner. This document describes the required information services along with the certificate mechanism that will be required for the support of such information services in a gaming environment.

In support of the certificate authority, several new uses for authentication and encryption will be introduced, as well as the new utilization of the ITU-T X509 authentication framework.

The consequence of the new gaming information system is a cryptographicaly secure relationship between physically located gaming machines in a casino. Such a relationship will also allow casino games to be seemlessly extended to the Internet using cryptographically secure means. In particular, there is no certificate authorities in use by casinos and local games.

Introduction

In order to achieve a framework that satisfies the information security goals associated with modern gaming and electronic commerce, there needs to be an infrastructure that can maintain a collection of keys. Modern cryptographic functions rely upon keys to protect and unprotect information. More generally, cryptographic protocols and primitives use these keys to achieve each of the information security objectives. Because of the way digital information can be replicated without owner consent, the keys should be regarded as the secret. If this is the case, we now have a new problem of where and how to store the keys so that the information the keys protect is not compromised.

Until about 1974, the primary means for encrypting information to protect privacy used symmetric key techniques. Soon after, however, it was observed that public-key methods could solve the key update problem between two users that know each other. Getting two strangers to have confidence in the identity of each other and content of a transaction, however, was soon seen to be a problem. Digital signature and certificate authorities often rely upon public key cryptography and were developed to solve some of the problems that untrusting parties face when engaging in digital commerce. In the next section, we generally define symmetric and public-key methods, their relative strengths, and weaknesses.

Information Security Goals

There are three goals of information security that are facilitated by cryptography: privacy, authentication, and non-repudiation. Providing a collection of services that satisfy these goals has been generally regarded as a necessary condition for a successful digital framework for electronic commerce. We make the same assumption about electronic gaming.

Privacy

Confidentiality or privacy is the condition where information is kept secret from all but those authorized to know the information. Encryption techniques will be used to ensure confidentiality. It should be noted that encryption does not necessarily provide authentication. Privacy can apply to individuals as well as information. Anonymous WWW surfing is an example of a problem requiring identity confidentiality. Game players may require that their identity not be divulged as a precondition for play. Confidentiality provides this service.

Authentication

Ensuring the identity of communicating parties to one another is called user authentication. Ensuring the content, integrity, origin, date of origin, time sent and other attributes of a message is called message authentication. Authentication will be provided by combining hashing techniques with other cryptographic primitives to form more complicated structures called protocols.

Non-Repudiation

Preventing a party from denying previous actions or commitments is known as the non-repudiation problem. The digital signature can be used to verify the identity of participants in a transaction and later enforce non-repudiation. A casino will need the services of non-repudiation if it is to enforce payment by players that have wagered and lost.

Public and Private Keys

Symmetric-key cryptography, also known as secret-key cryptography, uses a unique key to exchange information between two parties. Therefore, the sender and the recipient of a message must share a secret, namely the key. The difficulty with this approach occurs when a key is compromised or when the parties would like to introduce a new key. This is known as the key-update problem. A well known secret-key cryptography algorithm is the Data Encryption Standard (DES), which is used by financial institutions to encrypt PINs (personal identification numbers).

Asymmetric-key cryptography, or public-key cryptography, by contrast uses two different keys for each participant in a transaction. The asymmetric key pair consists of a public and private-key. The two keys are mathematically related so that data encrypted with either key can only be decrypted using the other. The public-key is made available to the world, while the private-key is kept secret. Entities desiring to send information to a particular individual will obtain the individual's public-key and encrypt information with that key. Only the holder of the private-key can then decrypt the information. This assurance is dependent upon not disclosing the private-key to anyone else. The essential feature of a public-key cryptosystem is that *knowledge of a public-key does not provide any computational information about the private-key.* One well-known public-key cryptography algorithm is RSA (named after its inventors Rivest, Shamir, and Adleman).

Cryptographic Background Art

This section lists four patents that provide the foundational art for public-key cryptography.

Patent number 5,231,668, the Digital Signature Algorithm (DSA). The DSA patent discusses signature schemes in a public-key context.

Patent 4,200,770, the Diffie-Hellman. The Diffie-Hellman patent is an important public-key patent and the described methods are often used for exchanging keys privately over a public network.

Patent 4,405,829, the RSA patent. The RSA patent describes the de-facto standard for public-key encryption around the world.

Patent 4,995,082, the Schnoor identification scheme. Schnoor developed an identification scheme that was later improved by the DSA patent. This patent then becomes prior art for the DSA patent.

Certificates

A certificate authority (CA) is a trusted third-party organization or company that can issues digital certificates used to create digital signatures and public-private key pairs. A public-key (CA) is required whenever a distributed application makes use of public-key cryptography. There are symmetric-key certificate authorities, but we will not consider them in this document. The term certificate authority, or CA, will be used to mean public-key certificate authority. The role of the CA is to guarantee that identity of the individual granted a unique certificate. Usually, this means that the CA has an arrangement with a financial institution, such as a credit card company, which provides it with information to confirm an individual's claimed identity. CAs are a critical component in data security and electronic commerce because the CA can be used to guarantee the identity of two parties exchanging information.

Simple Authentication

Strong Authentication

Certificates

A Heirarchy of Certificate Authorities

Alcorn 086'

The Alcorn 086 patent describes a public key authentication program for verification of the contents a hard disk and therefore a stored game. The use of authentication and encryption programs are not used for the confidentiality and integrity of the digital information that is transferred back and forth between gaming machines, such as a slot machine and a casino server. As such, the present patent describes new art.

Keene EP 0843 289 A2

1. Action Item for Bob: We need an engineer to look at figures 2A, 2B, and 4, 5 to ensure that they somehow don't do what we are suggesting with the array.

Can't claim parity bias solution

2. Action Item for Me: Discuss Blum-Micali (crypt. + secure)

The Keen patent uses a noise diode to facilitate the generation of random numbers. These random numbers are then used in game play. There are well-documented difficulties with obtaining randomness from physical noise sources, such as zener diodes. The problems with these physical sources of randomness include bias and correlation in the output bits [1]. Despite their shortcomings, there are advantages to physical noise sources as opposed to deterministic pseudo-random number generators. One advantage is that no seed is required. Another advantage is that a higher sampling rate can be achieved. We will examine two classes of problems that require random number generation in gaming: seed generation, and sequence generation.

No bias mention in Keene

Pseudo-random number generators from deterministic algorithms require a seed, or initial value. Random seeds to be used in a random number generator must be chosen with care otherwise there is a danger that any dependence in the bits of the seed can become amplified in the bits of the pseudo random number generator and lead to an adversary discovering information about the sequence that is used in a game. We discuss a scheme where a collection of physical sources can be used either as a seed for a pseudo-random generator, or simply as

Figs. 2a - 2b - 4 - 5

a generator for a sequence of random numbers. There is no need to provide seeds for systems that incorporate such number generators, thus simplifying the complexity of maintenance of the gaming machines.

A first solution to the problem of using physical sources of randomness that exhibit bias for random number generation, is to use process 700 from the Universal Gaming Engine to filter the bit streams that exhibit noise and correlation. One advantage of using the UGE filtering mechanism embodied in process 700 is that the device user can then decide on what time scale they would like to obtain stationarity in the output distribution. Using process 700, it is possible to verify that the output sequence of random numbers that will be used later in game play satisfy a collection of criteria that becomes a measure for the quality of the numbers. This measure is often noise generated numbers are statistically random. Having an apparatus such as given in process 700 of the UGE patent (fig. 7) should be a requirement of each random number system approved by a gaming commission. One difficulty, however, with using process 700 of the UGE to filter out correlated or biased sequences is that if the generator does exhibit sufficient bias then play might halt due to a shortage of random numbers.

A further improvement in the solution to this problem of using physical sources for randomness is found in the arrangement of the physical sources. By organizing several physical sources into a particular model we can take the output of the physical sources of randomness, considered semi-random sources; and produce a high quality output of randomness: a quasi-random source. It has been shown that such quasi-random sources can be used in place of truly random ones for applications such as random number generation and random number seed generation [2].

Suppose that we have a source of some randomness that exhibits a bias that is greater than δ and less than $1-\delta$ for some positive number $0<\delta<1$. Let us define a semi-random source as one in which the frequency of the 0's and 1's drifts over time with this bias. Zener diodes fall into the category of semi-random sources.

One construction of a quasi-random source from a semi-random source proceeds as follows. Let n be the input and suppose that we have k independent semi-random sources. Suppose that we then generate the following collection of bit lists:

$$\begin{array}{llll} X_{11} & X_{12} & \ldots & X_{1n} \\ X_{21} & X_{22} & \ldots & X_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ X_{k1} & X_{k2} & \ldots & X_{kn} \end{array}$$

Let Y_i = Parity $(X_{1i}, X_{2i}, \ldots, X_{ki})$ then the output $Y_1, Y_2, \ldots, Y_n$ is quasi-random. Even though such a sequence generates a high-quality source of randomness, it is still beneficial to ensure the integrity of the system by passing the resulting stream through process 700 of the UGE.

The solution that results does not significantly raise the hardware costs and needs only focus on ensuring the physical independence of the k semi-random sources by isolating the sources from electromagnetic interaction.

[1] J. Von Neumann, Various techniques used in connection with random digits (notes by G.E. Forsythe), Applied Math Series Vol. 12, pp. 36-38, 1951; National Bureau of Standards, Washington, D.C., reprinted in "Collected Works", Vol. 5, 768-770, Pergamon, New York, 1963.

[2] M. Santha and U. Vazirani, Generating Quasi-random Seque3nces from Semi-random Sources, Journal of Computer and System Sciences 33, 75-87 (1986).

From: Charles McCrea, Jr. <CharlieM@mikohn.com>
To: 'Bob Dorr' <bobdorr@sni.net>
Cc: Dave Thompson <DaveT@mikohn.com>
Date: Monday, March 15, 1999 10:29 AM
Subject: RE: Innovative Gaming 3/12/99

Bob,

Please proceed with Rolf's patent applicatiions.

Charlie

-----Original Message-----
From: Bob Dorr [SMTP:bobdorr@sni.net]
Sent: Friday, March 12, 1999 9:17 AM
To: Aaron Passman; Charles McCrea, Jr.; Rölf Carlson
Subject: I

Pl es on

REDACTED

Charlie, we are still awaiting authorization on Rolf's patent applications. << File: rolf7.REF >>

From: Bob Dorr <bobdorr@sni.net>
To: rolfc@swcp.com <rolfc@swcp.com>
Date: Thursday, April 01, 1999 2:50 PM
Subject: Re: Papers in the Mail

Hi Rolf,
I received the papers today and gave them to John. Thanks Bob
-----Original Message-----
From: Rolf Carlson <rolfc@swcp.com>
To: Robert Dorr (E-mail) <bobdorr@sni.net>
Date: Wednesday, March 31, 1999 4:56 AM
Subject: Papers in the Mail

>Hi Bob,
>
>You should receive a package from me in the next few days with the papers
>that support our patent applications.
>
>Rolf
>
>===================================
>Rolf Carlson
>Phone: (505) 857-0710
>Fax: (505) 822-0883
>rolfc@swcp.com
>http://www.swcp.com/~rolfc/
>

John Thompson

From: Rolf Carlson <rolfc@swcp.com>
To: John Thompson (E-mail) <jthompson@patnet.com>
Sent: Tuesday, July 13, 1999 8:24 PM
Subject: Patent and Presentation

Hi John,

How is the Certificate Authority patent coming along? I'd like to start putting that presentation together on both the UGE and Certificate Authority Patent so we can brief Mikohn. I'll send you a draft by the end of the week on the presentation. Is your time clear to start looking at the presentation in addition to working on the Certificate Authority Patent?

Rolf

====================================
Rolf Carlson
Phone: (505) 857-0710
rolfc@swcp.com

John Thompson

From: John Thompson <jthompson@patnet.com>
To: <rolfc@swcp.com>
Sent: Wednesday, July 14, 1999 9:18 AM
Subject: Re: Patent and Presentation

Rolf,

The revision of the patent application is coming along fine. We have revised the claims and drawings. We are in the middle of the revision of the specification. I should finish the revision of the specification by Thursday and then Bob will review the revised specification. I believe that we should have a draft to you by early next week.

Please feel free to send the presentation. I will review it and provide you with any comments or additional information that you need.

In addition, we have received an Office Action from the Patent Office with

REDACTED

Thanks for your email and I will be talking to you on Friday.

John F. Thompson
Dorr, Carson, Sloan and Birney
3010 East Sixth Ave.
Denver, CO 80206

(303) 333-3010
FAX (303) 333-1470

NOTICE OF CONFIDENTIALITY
This E-MAIL is intended only for the individual to whom it is addressed and contains information that is attorney-client privileged and/or confidential. If you have received this E-MAIL in error, please notify Dorr, Carson, Sloan & Birney, P.C. immediately by telephone (collect @ 303-333-3010) and please delete any copies of this E-MAIL. Any review, disclosure, copying, dissemination, or taking any action in reliance on any information contained herein is FORBIDDEN! Thank you.

----- Original Message -----
From: Rolf Carlson <rolfc@swcp.com>
To: John Thompson (E-mail) <jthompson@patnet.com>
Sent: Tuesday, July 13, 1999 8:24 PM
Subject: Patent and Presentation

> Hi John,
>
> How is the Certificate Authority patent coming along? I'd like to start
> putting that presentation together on both the UGE and Certificate
Authority

> Patent so we can brief Mikohn. I'll send you a draft by the end of the
week
> on the presentation. Is your time clear to start looking at the
> presentation in addition to working on the Certificate Authority Patent?
>
> Rolf
>
> ==================================
> Rolf Carlson
> Phone: (505) 857-0710
> rolfc@swcp.com

DORR, CARSON, SLOAN & BIRNEY, P.C.

Robert C. Dorr
W. Scott Carson
Jack C. Sloan
Thomas S. Birney

Leslie P. Kramer
John F. Thompson

The Patent Law Building
3010 East 6th Avenue
Denver, Colorado 80206

(303) 333-3010
FAX (303) 333-1470

Of Counsel:
Christopher H. Munch
Steve A. Mains

August 25, 1999

Rolf Carlson
Spring Creek Technologies, Corp.
5309 C Heritage Way NE
Albuquerque, NM 87109

Re: Draft U.S. Patent Application entitled "CRYPTOGRAPHY AND CERTIFICATE AUTHORITIES IN GAMING MACHINES"
Docket No. 1482/246

Dear Rolf:

Enclosed please find a first draft of the above-entitled patent application. I have also emailed a copy of the text to you. Please carefully review the patent application and verify that each statement is technically correct. Please feel free to make any additions or deletions that you believe are necessary for proper understanding of the invention.

The patent application must set forth sufficient detail for one skilled in the art to construct your system without undue experimentation. Furthermore, the disclosure must represent the best mode as of the date of filing. These are strict legal requirements which must be adhered to and, if not, the validity of any issuing patent may be affected.

Please carefully study the claims at the end of the application. Also remember that the claims, if allowed, will represent the legal monopoly. Therefore, it is important that you understand them.

In addition, we would like any written information or publications that you have that show the prior devices that are described in the background section of the application so that we may submit these documents to the Patent Office.

Also note that we represent Mikohn Gaming in this matter, and we do not represent you personally.

If you have any questions or comments, please contact me.

Sincerely yours,

DORR, CARSON, SLOAN & BIRNEY, P.C.

By: ______________________
John F. Thompson

C:\Client\1482 Mikohn\-246\Carlson ltr1.doc

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/698,507	10/26/2000	Rolf E. Carlson	xRCa-12	3367

20995 7590 01/13/2005

KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614

EXAMINER	
HOFFMAN, BRANDON S	
ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 01/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/698,507	**Applicant(s)** CARLSON, ROLF E.
	Examiner Brandon Hoffman	**Art Unit** 2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 January 2005*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-60 and 62-71* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-60 and 62-71* is/are rejected.

7)☒ Claim(s) *62-71* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 October 2000* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Miscellaneous Matters

1. In response to the phone interview with applicant's representative, Ms. Metcalf, on January 6, 2005, a second copy of the non-final office action (originally sent December 1, 2004) is being sent. A change in power of attorney and correspondence address was submitted on November 24, 2004, but due to processing time, the action was sent to the old address. Therefore, the action is being resent to the updated address with a new period for response date.

Specification

2. The disclosure is objected to because of the following informalities:

- On page 3, lines 24, "exits" should be –exists–.

3. The numbering of claims is not in accordance with 37 CFR 1.126 which requires the original numbering of the claims to be preserved throughout the prosecution. When claims are canceled, the remaining claims must not be renumbered. When new claims are presented, they must be numbered consecutively beginning with the number next following the highest numbered claims previously presented (whether entered or not).

Misnumbered claims 62-71 shall be renumbered 61-70, respectively.Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Karmarkar (U.S. Patent No. 6,508,709) in view of MacKenzie et al. (U.S. Patent No. 6,757,825).

Regarding claim 1, Karmarkar teaches a casino gaming system, comprising:

- At least one gaming machine (fig. 1C, ref. num 46);
- A gaming server including a plurality of keys (fig. 1B, ref. num 10); and
- A network bus interconnecting said at least one gaming machine and said gaming server, said network bus used to transmit information between said at least one gaming machine and said gaming server (fig. 1B, ref. num 44 and 48),
- Said at least one gaming machine using said at least one of said plurality of keys to encrypt said information (fig. 14B, ref. num 646) and
- Said at least one gaming machine transmitting said encrypted information over said network bus (fig. 14B, ref. num 648).

Karmarkar does not teach said gaming server transmitting at least one of said plurality of keys over said network bus to said at least one gaming machine.

MacKenzie et al. teaches said gaming server transmitting at least one of said plurality of keys over said network bus to said at least one gaming machine (col. 3, lines 8-11).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine said gaming server transmitting at least one of said plurality of keys over said network bus to said at least one gaming machine, as taught by MacKenzie et al., with the system of Karmarkar. It would have been obvious for such modifications because transmitting the server's public key will provide the recipients the proper encryption key to encrypt their data. The server can then use its private key to decrypt the data.

Regarding claim 17, Karmarkar teaches a casino gaming system, comprising:

- A plurality of gaming machines (fig. 1C, ref. num 46);
- A gaming server (fig. 1B, ref. num 10) comprising: each of said plurality of keys including a time stamp, said time stamp indicating a period of time for which each of said plurality of keys is used; a random number generator that generates said plurality of keys; and an encryption algorithm (col. 6, lines 59-65 and col. 12, lines 35-37),

- A network bus interconnecting said plurality of gaming machines and said gaming server, said network bus used to transmit information between said plurality of gaming machines and said gaming server (fig. 1B, ref. num 44 and 48),
- Said gaming server transmitting said at least one of said plurality of keys over said network bus to at least one of said plurality of gaming machines where said key is decrypted (fig. 14A, ref. num 630 and 632),
- Said at least one of said plurality of gaming machines using said at least one of said plurality of keys to encrypt said information (fig. 14B, ref. num 646),
- Said at least one of said plurality of gaming machines transmitting said encrypted information over said network bus (fig. 14B, ref. num 648).

Karmarkar does not teach the gaming server comprising a plurality of keys, said gaming server using said encryption algorithm to encrypt at least one of said plurality of keys.

MacKenzie et al. teaches the gaming server comprising a plurality of keys, said gaming server using said encryption algorithm to encrypt at least one of said plurality of keys (col. 3, lines 8-11).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the gaming server comprising a plurality of keys, said gaming server using said encryption algorithm to encrypt at least one of said plurality of keys, as taught by MacKenzie et al., with the system of Karmarkar. It would have been obvious for such modifications because transmitting the server's public key will provide the recipients the proper encryption key to encrypt their data. The server can then use its private key to decrypt the data.

Regarding claim 25, Karmarkar teaches a method for communicating information using a casino gaming system having at least one gaming machine and a gaming server, said method comprising the steps of:

- Establishing a first communication link between said at least one gaming machine and said gaming sever (fig. 1B, ref. num 44);
- Encrypting information sent from said at least one gaming machine using said at least one of said plurality keys (fig. 14B, ref. num 646);
- Second transmitting said encrypted information over said first communication link from said at least one gaming machine (fig. 14B, ref. num 648); and
- Decrypting said received encrypted information (fig. 14A, ref. num 650).

Karmarkar does not teach first transmitting at least one of a plurality of keys stored at said gaming server over said first communication link from said gaming server to said at least one gaming machine.

MacKenzie et al. teaches first transmitting at least one of a plurality of keys stored at said gaming server over said first communication link from said gaming server to said at least one gaming machine (col. 3, lines 8-11).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine first transmitting at least one of a plurality of keys stored at said gaming server over said first communication link from said gaming server to said at least one gaming machine, as taught by MacKenzie et al., with the method of Karmarkar. It would have been obvious for such modifications because transmitting the server's public key will provide the recipients the proper encryption key to encrypt their data. The server can then use its private key to decrypt the data.

Regarding claims 2, 18, and 26, the combination of Karmarkar in view of MacKenzie et al. teaches wherein said plurality of keys are symmetric keys (see col. 6, lines 59-65 of Karmarkar).

Regarding claims 3, 19, and 27, the combination of Karmarkar in view of MacKenzie et al. teaches wherein said symmetric keys are session keys (see col. 5, lines 39-42 of MacKenzie et al.).

Regarding claim 4, the combination of Karmarkar in view of MacKenzie et al. teaches wherein said symmetric keys comprise Data Encryption Standard (DES) algorithms (see col. 6, lines 59-65 of Karmarkar).

Regarding claim 5, the combination of Karmarkar in view of MacKenzie et al. teaches wherein said symmetric keys comprise triple Data Encryption Standard (triple-DES) algorithms (see col. 12, line 28 of Karmarkar).

Regarding claims 6, 20, and 28, the combination of Karmarkar in view of MacKenzie et al. teaches wherein said plurality of keys comprise asymmetric key pairs (see col. 6, lines 59-65 of Karmarkar).

Regarding claims 7, 21, and 29, the combination of Karmarkar in view of MacKenzie et al. teaches wherein said asymmetric keys are session keys (see col. 5, lines 39-42 of MacKenzie et al.).

Regarding claim 8, the combination of Karmarkar in view of MacKenzie et al. teaches wherein said asymmetric key pairs comprise Rivest, Shamir, and Adleman (RSA) algorithms (see col. 6, lines 59-65 of Karmarkar).

Regarding claims 9 and 30, the combination of Karmarkar in view of MacKenzie et al. teaches wherein said gaming server is interconnected to an outside network (see fig. 1C, ref. num 52 of Karmarkar).

Regarding claims 10 and 31, the combination of Karmarkar in view of MacKenzie et al. teaches wherein said outside network is the Internet (see fig. 1C, ref. num 52 of Karmarkar).

Regarding claim 11, the combination of Karmarkar in view of MacKenzie et al. teaches wherein each of said plurality of keys includes a time stamp, said time stamp indicating a period of time for which each of said plurality of keys is used (see col. 12, lines 35-37 of Karmarkar).

Regarding claims 12 and 32, the combination of Karmarkar in view of MacKenzie et al. teaches wherein said gaming server further comprises a random number generator that generates said plurality of keys (see col. 8, line 64 through col. 9, line 4 of Karmarkar).

Regarding claim 13, the combination of Karmarkar in view of MacKenzie et al. teaches said gaming server further comprising:

- An encryption algorithm, said gaming server using said encryption algorithm to encrypt said at least one of said plurality of keys (see col. 6, lines 59-65 of Karmarkar),
- Said gaming server transmitting said encrypted at least one of said plurality of keys over said network bus to said at least one gaming machine (see col. 3, lines 8-11 of MacKenzie et al.).

Regarding claims 14 and 22, the combination of Karmarkar in view of MacKenzie et al. teaches wherein said encrypted information is transmitted over said network bus to another of said at least one gaming machines (see col. 23, lines 10-12 of Karmarkar).

Regarding claims 15 and 23, the combination of Karmarkar in view of MacKenzie et al. teaches wherein said encrypted information is transmitted over said network bus to said gaming server (see fig. 14B, ref. num 646-650 of Karmarkar).

Regarding claims 16 and 24, the combination of Karmarkar in view of MacKenzie et al. teaches further comprising:

- An outside network connected to said gaming server (see fig. 1C, ref. num 52 of Karmarkar); and
- A remote computer connected to said outside network wherein said encrypted information is transmitted over said network bus and said outside network to said remote computer (see fig. 1C, ref. num 54 of Karmarkar).

Regarding claim 33, the combination of Karmarkar in view of MacKenzie et al. teaches further comprising the steps of encrypting each of said plurality of keys transmitted from said gaming server to said at least one gaming machine (see col. 3, lines 8-11 of MacKenzie et al.).

Regarding claim 34, the combination of Karmarkar in view of MacKenzie et al. teaches wherein said step of second transmitting further comprises transmitting said encrypted information over said first communication link to another of said at least one gaming machine, and wherein said step of decrypting further comprises decrypting said received encrypted information at said another of said at least one gaming machine (see col. 23, lines 10-12 and fig. 14B, ref. num 632 of Karmarkar).

Regarding claim 35, the combination of Karmarkar in view of MacKenzie et al. teaches wherein said step of transmitting further comprises second transmitting said encrypted information over said first communication link to said gaming server, and wherein said step of decrypting further comprises decrypting said received encrypted information at said gaming server (see fig. 14A, ref. num 650 of Karmarkar).

Regarding claim 36, the combination of Karmarkar in view of MacKenzie et al. teaches further comprising the step of establishing a second communication link between said gaming server and a remote computer (see fig. 1C, ref. num 52 and 54 of Karmarkar).

Regarding claim 37, the combination of Karmarkar in view of MacKenzie et al. teaches wherein said step of transmitting further comprises transmitting said encrypted information over said first communication link and said second communication link to said remote computer, and wherein said step of decrypting further comprises decrypting said received encrypted information at said remote computer (see fig. 14A, ref. num 630 and fig. 14B, ref. num 632 of Karmarkar).

Claims 38-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Karmarkar (USPN '709) in view of Van Oorschot (U.S. Patent No. 6,370,249).

Regarding claim 38, Karmarkar teaches a casino gaming system for communicating information using asymmetric key pairs that includes a private key and a public key, said casino gaming system comprising:

- A plurality of gaming machines (fig. 1C, ref. num 46);
- A network bus interconnecting said plurality of gaming machines and said certificate authority server (fig. 1B, ref. num 44 and 48),
- Said at least one of said plurality of gaming machines using said at least one of said plurality of said public keys to encrypt information (fig. 14B, ref. num 646),
- Said at least one of said plurality of gaming machines transmitting said encrypted information over said network bus (fig. 14B, ref. num 648).

Karmarkar does not teach a certificate authority server including a memory storing at least a plurality of said public keys of said asymmetric key pairs, said certificate authority server transmitting at least one of said plurality of public keys over said network bus to at least one of said plurality of gaming machines wherein said certificate authority server signs said at least one of said plurality of public keys transmitted over said network bus.

Van Oorschot teaches a certificate authority server including a memory storing at least a plurality of said public keys of said asymmetric key pairs (fig. 1, ref. num 72), said certificate authority server transmitting at least one of said plurality of public keys over said network bus to at least one of said plurality of gaming machines wherein said certificate authority server signs said at least one of said plurality of public keys transmitted over said network bus (col. 3, lines 13-33).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a certificate authority server including a memory storing at least a plurality of said public keys of said asymmetric key pairs, said certificate authority server transmitting at least one of said plurality of public keys over said network bus to at least one of said plurality of gaming machines wherein said certificate authority server signs said at least one of said plurality of public keys transmitted over said network bus, as taught by Van Oorschot, with the system of Karmarkar. It would have been obvious for such modifications because a certificate authority enables to gaming machine to 'trust' the public keys being received. In a non-certificate authority environment, the gaming machine (client) has to perform additional authentication with the server in order to obtain the same trust level as with the certificate authority. This saves time, which is especially important in a real-time application.

Regarding claim 39, the combination of Karmarkar in view of Van Oorschot teaches wherein each of said plurality of gaming machines validates said at least one of said signed plurality of public keys received from said network bus (see col. 1, lines 43-50 of Van Oorschot).

Regarding claim 40, the combination of Karmarkar in view of Van Oorschot teaches wherein said certificate authority server is connected to an outside network (see fig. 1C, ref. num 52 of Karmarkar).

Regarding claim 41, the combination of Karmarkar in view of Van Oorschot teaches wherein said outside network is the Internet (see fig. 1C, ref. num 52 of Karmarkar).

Regarding claim 42, the combination of Karmarkar in view of Van Oorschot teaches wherein said encrypted information is transmitted over said network bus to another of said at least one gaming machines (see col. 23, lines 10-12 of Karmarkar).

Regarding claim 43, the combination of Karmarkar in view of Van Oorschot teaches wherein said encrypted information is transmitted over said network bus to said gaming server (see fig. 14B, ref. num 646-650 of Karmarkar).

Regarding claim 44, the combination of Karmarkar in view of Van Oorschot teaches further comprising:

- An outside network connected to said gaming server (see fig. 1C, ref. num 52 of Karmarkar); and
- A remote computer connected to said outside network wherein said encrypted information is transmitted over said network bus and said outside network to said remote computer (see fig. 1C, ref. num 54 of Karmarkar).

Regarding claim 45, the combination of Karmarkar in view of Van Oorschot teaches wherein said network bus is connected to at least one gaming server, said certificate authority server transmitting at least one of said plurality of said public keys to said at least one gaming server, said gaming server encrypts information using said at least one of said plurality of said public keys, said gaming server transmits said encrypted information over said network bus (see fig. 6, ref. num 182 of Van Oorschot).

Regarding claim 46, the combination of Karmarkar in view of Van Oorschot teaches wherein said gaming server further comprises a random number generator that generates said plurality of keys (see col. 8, line 64 through col. 9, line 4 of Karmarkar).

Regarding claim 47, the combination of Karmarkar in view of Van Oorschot teaches wherein each of said plurality of keys includes a time stamp, said time stamp indicating a period of time for which each of said plurality of keys is used (see col. 12, lines 35-37 of Karmarkar).

Regarding claim 48, the combination of Karmarkar in view of Van Oorschot teaches wherein said network bus is connected to a plurality of other certificate authority servers (see fig. 2 of Van Oorschot), said certificate authority server transmitting at least one of said plurality of said public keys to said plurality of other certificate authority servers wherein said plurality of other certificate authority servers encrypts information using said at least one of said plurality of said public keys and transmits said encrypted information over said network bus (see fig. 2, ref. num 34, 46, and 58 of Van Oorschot).

Claims 49-60 and 62-71 are rejected under 35 U.S.C. 103(a) as being unpatentable over Karmarkar (USPN '709) in view of Matsumoto et al. (U.S. Patent No. 6,711,264).

Regarding claims 49 and 55-57, Karmarkar teaches a casino gaming system connected to at least one outside computer via an outside network, said casino gaming system comprising:

- A gaming server (fig. 1B, ref. num 10);
- A plurality of gaming machines located in a casino (fig. 1C, ref. num 46);
- A plurality of access switches, each one of said plurality of access switches individually connected to a different one of said plurality of gaming machines (col. 7, lines 20-42);
- A network bus connected to said gaming server and each of said plurality of access switches (fig. 1B, ref. num 44, 48);
- Said outside network connected to said gaming server (fig. 1C, ref. num 52),
- One of said plurality of access switches connecting one of said plurality of gaming machines and said outside computer over said outside network, so as to enable a remote player of said outside computer to play said one of said plurality of gaming machines (fig. 1C, ref. num 52, 54).

Karmarkar does not teach connecting the gaming machine to the access switch when said one of said plurality of gaming machines is idle.

Matsumoto et al. teaches connecting the gaming machine to the access switch when said one of said plurality of gaming machines is idle (col. 14, lines 17-32).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine connecting the gaming machine to the access switch when said one of said plurality of gaming machines is idle, as taught by Matsumoto et al., with the system of Karmarkar. It would have been obvious for such modifications because selecting an idle machine prevents errors from occurring on a machine that is being simultaneously used by two different people.

Regarding claims 58, 69, and 71, Karmarkar teaches a method for communicating with a plurality of gaming machines in a casino, said plurality of gaming machines connected to a gaming server, said method comprising the steps of:

- Receiving a request from an outside network for an identified one of said plurality of gaming machines, said request initiated by a remote player (fig. 14B, ref. num 604); and
- Providing a secured communication link between said outside network and said identified one of said plurality of gaming machines, so as to enable the remote player to play a casino game at said identified one of said plurality of gaming machines (fig. 1B, ref. num 48 and 50 and fig. 1C, ref. num 52 and 54).

Karmarkar does not teach waiting for an idle gaming machine, or delivering to said outside network a gaming machine unavailable message when said identified one of said plurality of gaming machines is in use.

Matsumoto et al. teaches waiting for an idle gaming machine and delivering to said outside network a gaming machine unavailable message when said identified one of said plurality of gaming machines is in use (col. 14, lines 17-32).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine waiting for an idle gaming machine and delivering to said outside network a gaming machine unavailable message when said identified one of said plurality of gaming machines is in use, as taught by Matsumoto et al., with the system of Karmarkar. It would have been obvious for such modifications because waiting for a machine to be idle prevents errors from occurring on a machine that is being simultaneously used by two different people.

Regarding claims 50 and 68, the combination of Karmarkar in view of Matsumoto et al. teaches wherein said outside network is the Internet (see fig. 1C, ref. num 52 of Karmarkar).

Regarding claim 51, the combination of Karmarkar in view of Matsumoto et al. teaches further comprising a certificate authority server connected to said network bus, said certificate authority server including a plurality of public keys of a plurality of asymmetric key pairs (see col. 21, lines 36-48 of Matsumoto et al.).

Regarding claim 52, the combination of Karmarkar in view of Matsumoto et al. teaches wherein said outside computer acquires one of said plurality of public keys from said certificate authority server via said outside network and said network bus, said outside computer using said one of said plurality of public keys to encrypt information transmitted to said one of said plurality of gaming machines over said outside network and said network bus (see col. 21, lines 36-54 of Matsumoto et al.).

Regarding claim 53, the combination of Karmarkar in view of Matsumoto et al. teaches wherein information communicated between said outside computer and said one of said plurality of gaming machines over said outside network and said network bus is encrypted using asymmetric key pairs (see col. 6, lines 59-65 of Karmarkar).

Regarding claim 54, the combination of Karmarkar in view of Matsumoto et al. teaches wherein information communicated between said outside computer and said one of said plurality of gaming machines over said outside network and said network bus is encrypted using symmetric keys (see col. 6, lines 59-65 of Karmarkar).

Regarding claim 59, the combination of Karmarkar in view of Matsumoto et al. teaches wherein said step of receiving a request further comprising the steps of entering player identification information; and providing said entered player identification information to a database (see fig. 14A, ref. num 608 and 610 of Karmarkar).

Regarding claim 60, the combination of Karmarkar in view of Matsumoto et al. teaches wherein said step of providing said entered player identification information further comprises the steps of:

- Comparing said entered player identification information to said database (see fig. 14A, ref. num 605 of Karmarkar); and
- Providing said secured communication link between said outside network and said identified one of said plurality of gaming machines if said entered identification information matches an entry in said database (see fig. 14A, ref. num 614 and below of Karmarkar).

Regarding claim 62, the combination of Karmarkar in view of Matsumoto et al. teaches wherein said entered player identification information is credit card information (see col. 24, line 26 of Karmarkar).

Regarding claim 63, the combination of Karmarkar in view of Matsumoto et al. teaches further comprising the steps of documenting information about the remote player (see col. 24, lines 15-67 of Karmarkar).

Regarding claim 64, the combination of Karmarkar in view of Matsumoto et al. teaches wherein said documented information comprises information about the remote player (see col. 24, lines 19-27 of Karmarkar).

Regarding claim 65, the combination of Karmarkar in view of Matsumoto et al. teaches wherein said documented information comprises a time for which the remote player plays said one of said plurality of gaming machines (see col. 12, lines 35-37 of Karmarkar).

Regarding claim 66, the combination of Karmarkar in view of Matsumoto et al. teaches wherein said documented information comprises a location from which the remote player is playing (see col. 23, lines 13-15 of Karmarkar).

Regarding claim 67, the combination of Karmarkar in view of Matsumoto et al. teaches wherein said documented information comprises an amount the remote player has wagered (see col. 21, lines 1-5 of Karmarkar).

Regarding claim 70, the combination of Karmarkar in view of Matsumoto et al. teaches wherein said plurality of gaming machines are located in a casino (see col. 5, line 66 through col. 6, line 1 of Karmarkar).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

1/6/05
AU2131

Brandon Hoff

BH

Notice of References Cited	Application/Control No. 09/698,507	Applicant(s)/Patent Under Reexamination CARLSON, ROLF E.
	Examiner Brandon Hoffman	Art Unit 2136 — Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-6,757,825	06-2004	MacKenzie et al.	713/169
	B	US-6,711,264	03-2004	Matsumoto et al.	380/283
	C	US-6,508,709	01-2003	Karmarkar, Jayant S.	463/42
	D	US-6,370,249	04-2002	Van Oorschot, Paul C.	380/277
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.